VIA C7-M Technical Overview

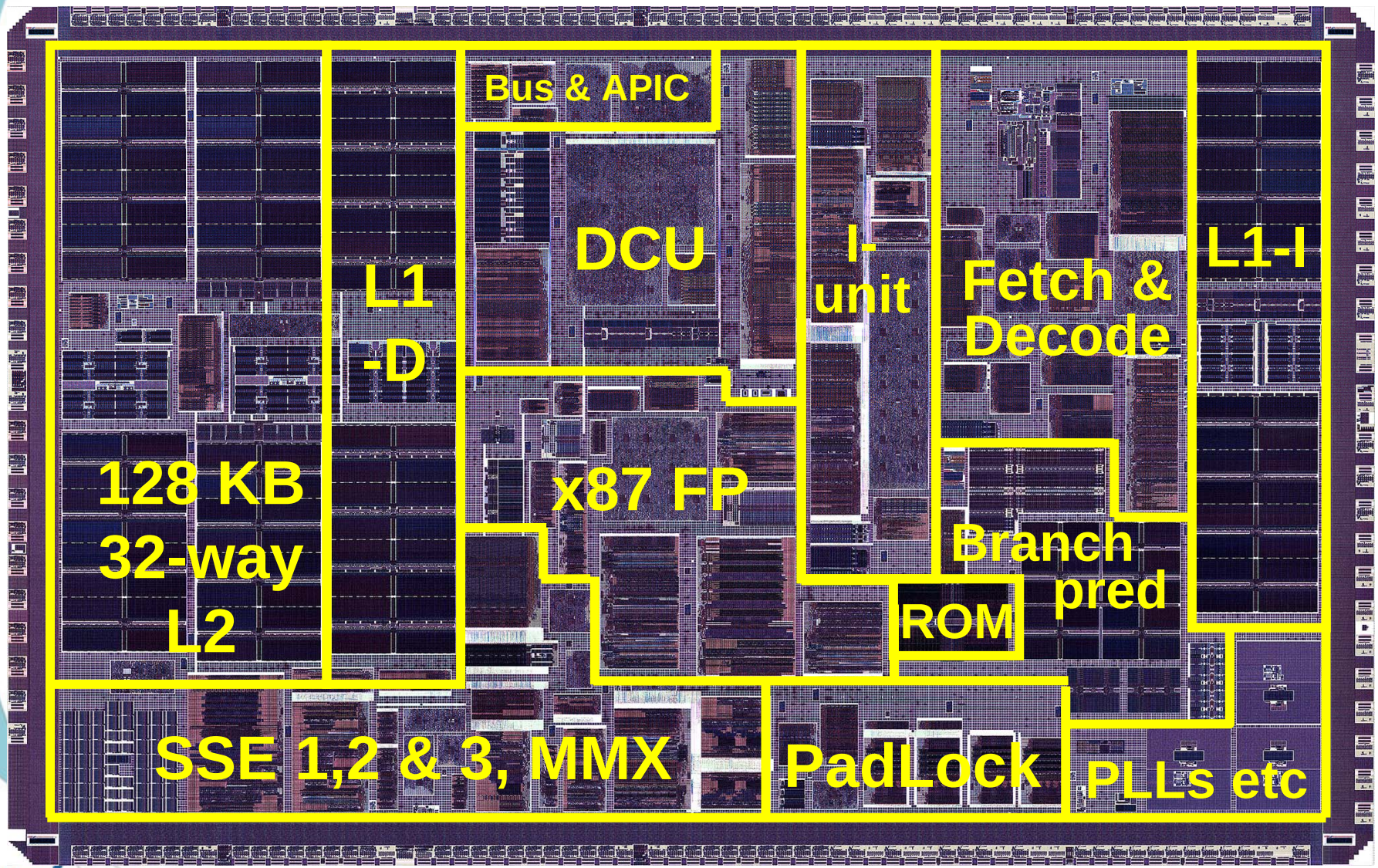
C.J. Holthaus
Centaur Technology

Enabling
Digital Brilliance

Centaur – VIA's Austin Design Center

- Led by Glenn Henry, former IBM Fellow and Dell CTO
- World-class team has created 18 CPU designs since 1995
- Design philosophy is to balance cost, power and performance

VIA C7 Processor: Elements

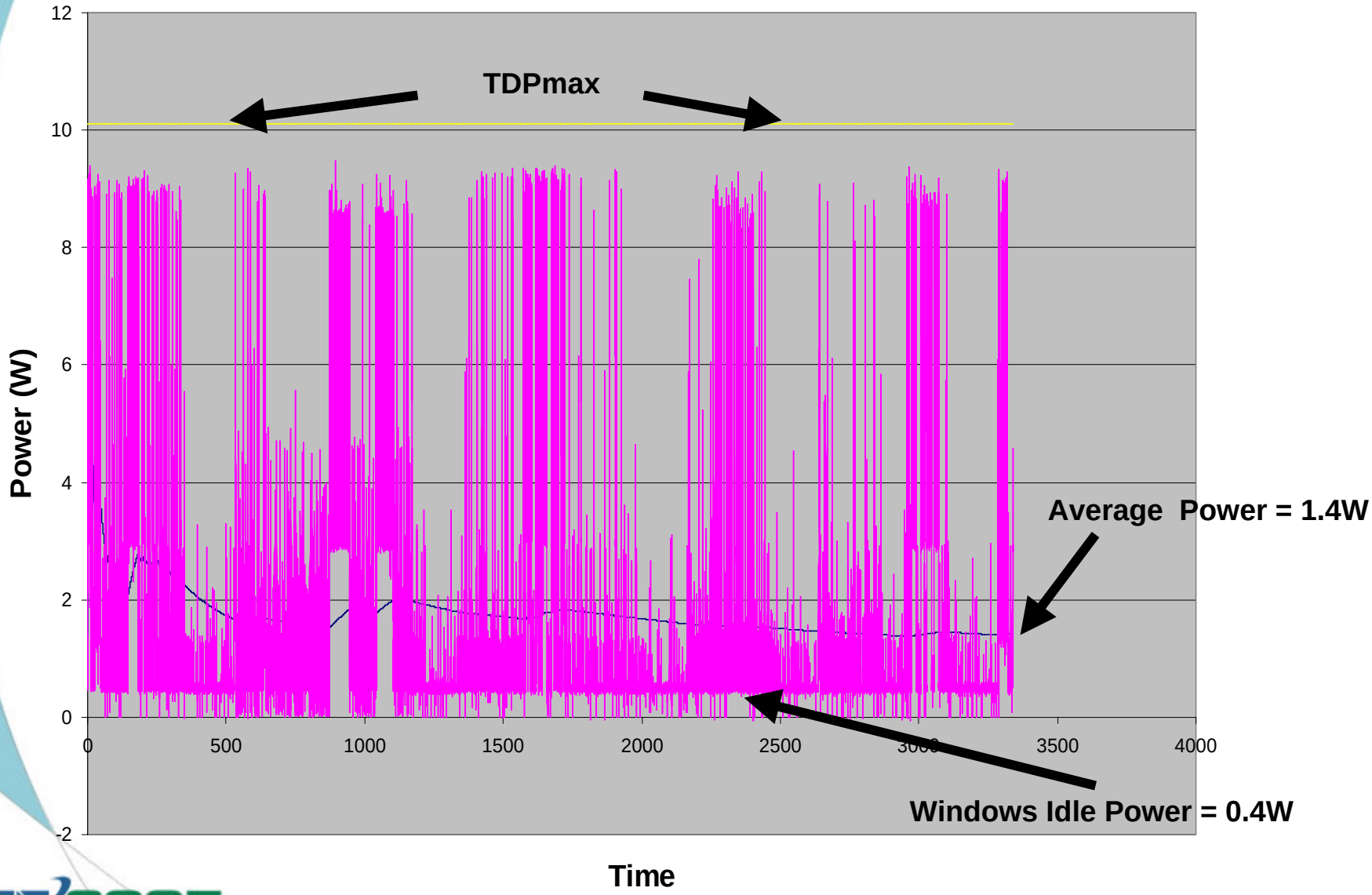


VIA C7-M Demonstration

VIA C7 - Designed for Mobility

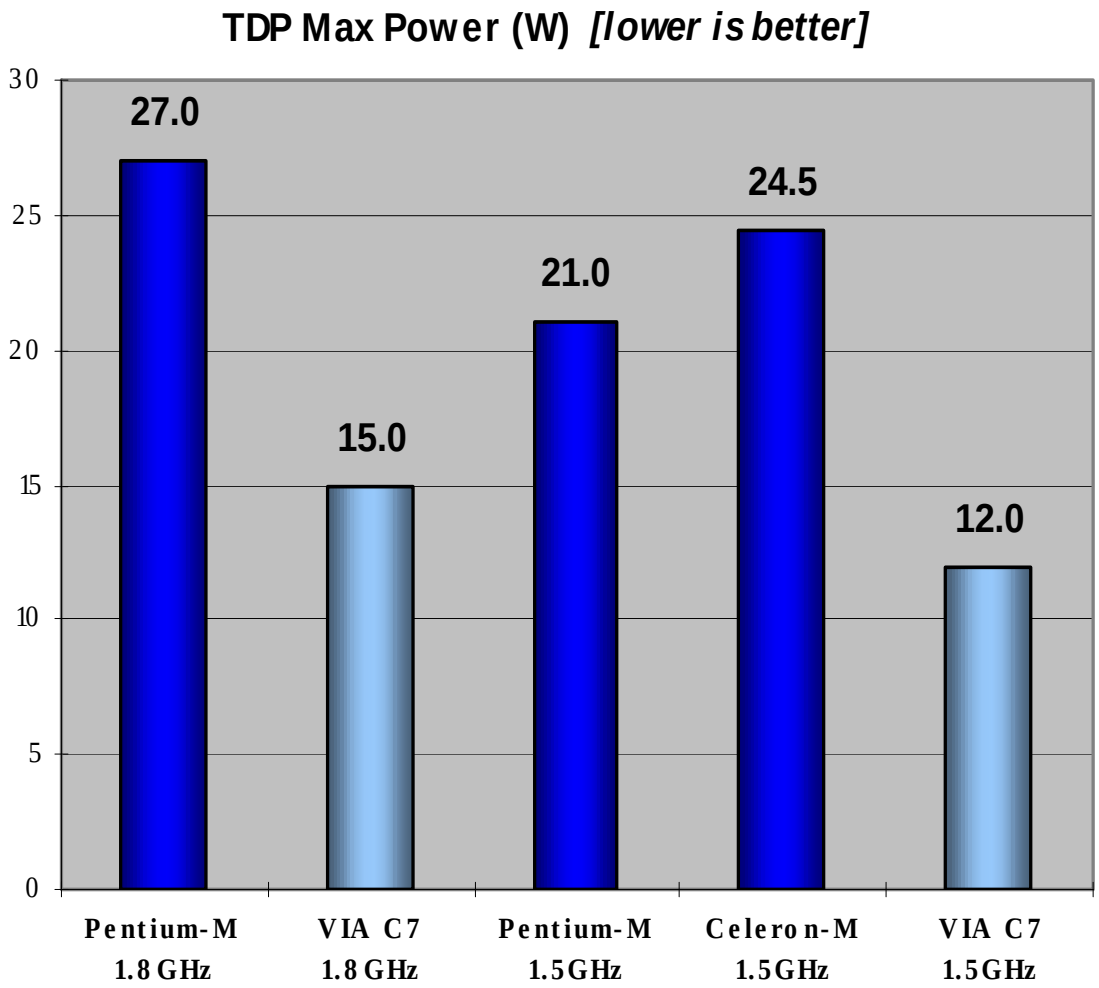
- Extends VIA leadership in reducing *MAXIMUM* power
  - Lower Thermal Design Point (TDP) to reduce the size and weight of cooling system
- Adds new features to reduce *AVERAGE* power
  - Rapidly accomplish computing tasks and then reduce power to minimize battery drain
- Increases performance on mobile applications
  - New features and speeds up to 2 GHz

VIA C7-M 1.5 GHz Power Profile



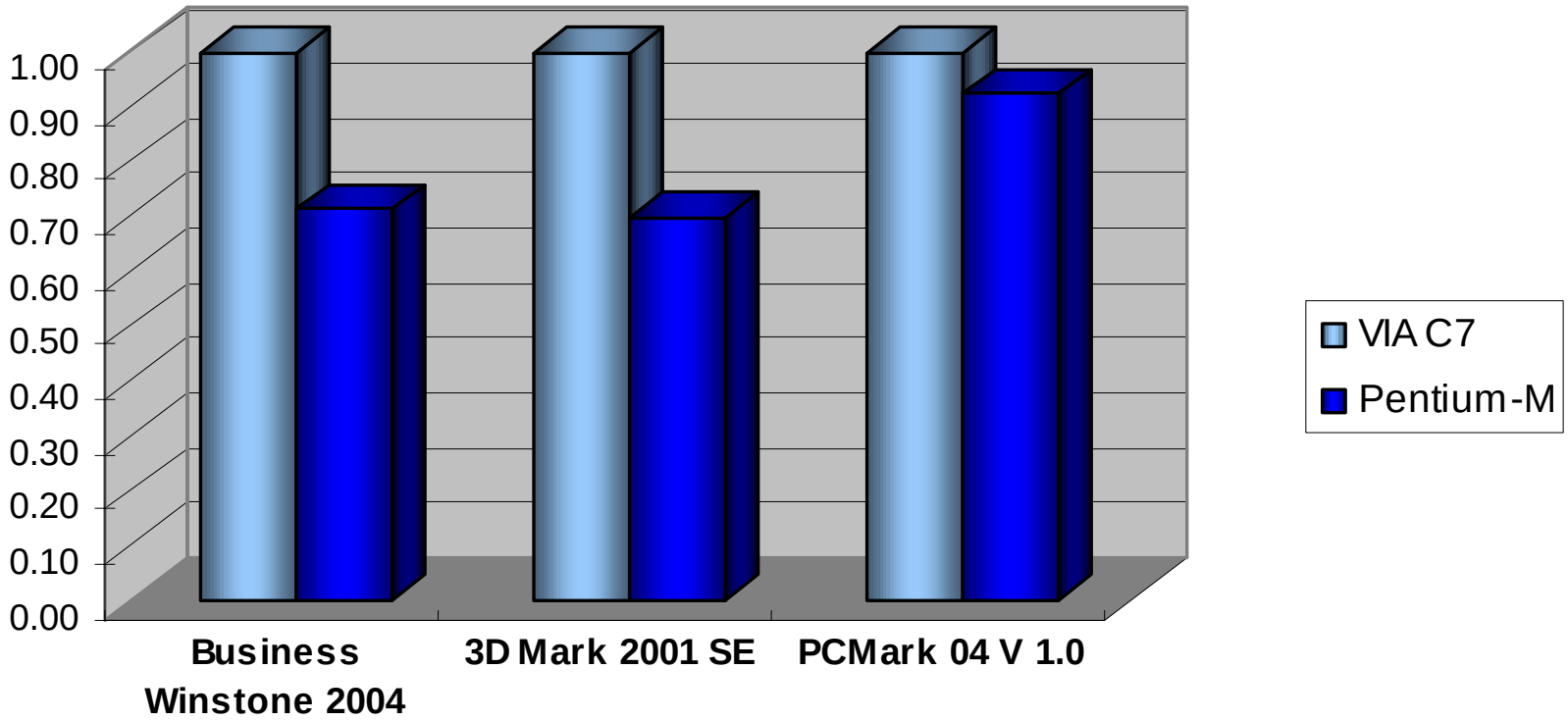
Low Power by Design

- Saves over 40% power compared with Intel® Pentium®-M
- Saves over 50% power compared with Intel® Celeron-M



Efficient by Design

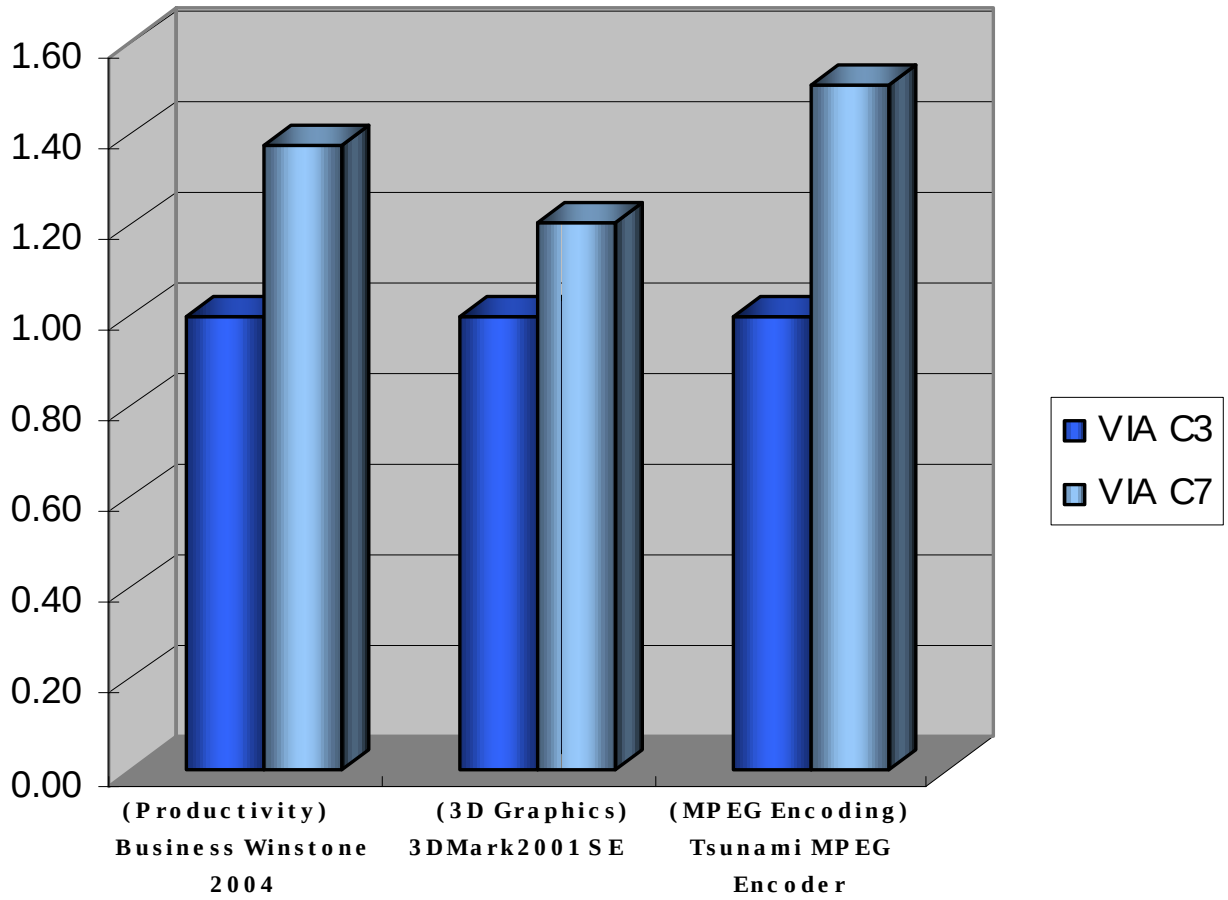
The VIA C7 delivers 15% better performance-per-watt than Intel® Pentium®-M at equivalent speed grade



* All benchmarks normalized to performance/TDPmax of the VIA C7-M processor@ 1.5GHz

Performance Enhancement

Major performance enhancement over previous VIA C3 generation at starting speed grades



*All benchmarks normalized to VIA C3

Enhanced PowerSaver™

- Power reduction technology using dynamic frequency and voltage adjustments
- Supported natively by Windows XP
- TwinTurbo PLL's
  - C7-M has two core clock PLL's for fastest frequency transitions
  - Snooping can occur during transitions
- Supports ACPI C0,C1,C2,C3,C4 states
- Low frequency and voltage
  - 600 MHz @ 0.908V

New VIA C7 TwinTurbo PLL

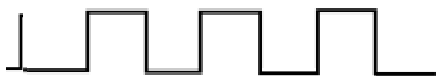
- Reduce User Response Time
  - Increase clock rate quickly if user activates a heavy compute workload
  - Decrease clock rate quickly after completing work in order to save power
- With a single PLL (Pentium M)
  - The CPU has to stop execution while shifting frequencies (P-States).
- VIA C7 Twin Turbo PLL
  - Uses a second PLL to switch P-States within 1 clock cycle

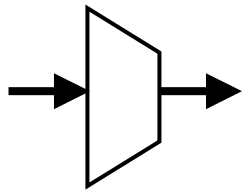
Twin Turbo PLL → Fast P-States

Pentium-M® P-State Transition

15000 Clock Delay!

Single PLL





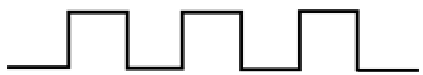
Change P-State

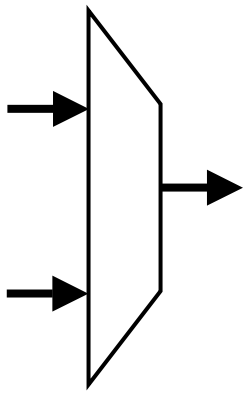
CPU and Bus Halted

VIA C7 P-State Transition

1 Clock Delay

Twin Turbo PLL





Change P-State

Designing for Power Efficiency

- While the CPU industry focused on performance at all costs: →

- Glenn Henry's team recognized the thermal wall approaching

- VIA CPU designs lead the industry move to focus on power efficiency

VIA C7™ Processor

Cool Processing!

VIA C7-M Details

- World class IBM Foundry using 90 nm SOI
- TDP-2.0 GHz @ ~20W and 1.0 GHz @ 3.0W
- nanoBGA2
  - Ultra small BGA 21mm x 21mm for lightest & thinnest notebooks
- With More Functionality:
  - SSE3
  - Up to 800 MHz FSB (1066 MHz possible)
    - Intel constrains FSB on Pentium-M to protect P4 positioning
  - Enhanced PowerSaver
    - Power reduction technology using dynamic frequency and voltage adjustments
    - TwinTurbo PLL's
      - C7-M has two core clock PLL's for fastest frequency transitions
      - Snooping can occur during transitions
  - Security features
    - SHA-1/256 & RSA modexp primitive
    - NX bit for memory protection.
      - It is not a panacea (萬能藥) for all virus types.
  - Dual and Quad processing

VIA C7-M Details

- Cache
  - 64k L1 Data (4-way) & 64k L1 Instruction (4-way)
  - 128k L2 (32-way,victim)
- Instruction Sets
  - SSE,SSE2,SSE3
  - VIA RNG, AES, SHA-1 SHA-256, RSA modexp
- Power Management
  - TwinTurbo PLL's for instantaneous P-state transitions
  - ACPI C0,C1,C2,C3,C4
- Thermal Features
  - Thermal Monitor 1-internal stop grant duty cycle
  - Thermal Monitor 2-changes to lowest P-state
  - Predefined & User-defined Threshold values
  - Catastrophic thermal protection

VIA C7-M

- Testability
  - Added JTAG-Boundary Scan (new to VIA processors)
- Compatibility
  - BIOS environment similar to other x86 processors
    - Standard MTRR's, APIC,SMM, etc.
    - Sample 1.5 GHz performance states:
      - 1.5 GHz @ 1.1V
      - 1.2 GHz @ 0.956V
      - 1.0 GHz @ 0.908V
      - 800 MHz @ 0.908V
      - 600 MHz @ 0.908V

High-Performance V4 Bus

- Advanced Bus Architecture Optimized for Streaming Data
  - Source-synchronous, allowing higher clock rates
  - Four 64-bit data transfers per clock
  - Smart Prefetching to maximize CPU throughput
- New Features not Available for P4 Bus
  - 50% Higher Write Bandwidth (overlaps write response cycle)
  - Sparse Write-Combining (Up to 15X faster pattern fills)
  - Linear Addressing Modes (flexibility for memory controller)
- Requires 20% Fewer Pins than P4 Bus
  - Uses 4 address cycles/clock, instead of only 2
- Supports 32-bit data mode for a 50% Pin Reduction over P4
- Data Clock Rates of 400/533MHz, scalable to over 1066MHz
  - Supports VIA roadmap to over 8.5 GBytes/sec bandwidth

Aspects of Security

Protection

- Safeguarding operating environment from malicious software

  Worms, Virii, DoS,et al.

Privacy

- Safeguarding sensitive information

  Symmetric Key and Public Key Encryption

Another Perspective

Securing the Automobile

Safety mechanisms

- Physical Protection

  Seat Belts, Airbags, Night vision

- Traffic rules and regulations

  License,Speed Limit, Lane restrictions

VIA Security Strategy

- Provide basic security primitives in the CPU
  - Hardware provides increased security & performance
  - On processor die better than on other chips
- No operating system support required
  - All function directly accessible by application
    Provided by new x86 instruction
  - Transparent multitasking provided by hardware
    No new state or control registers to save
  - Direct access provides increased security
- Built into all of our processors, for free
  - It's so small that our die size doesn't grow
- *Why… Security is/will be pervasive need,*
  Processor can do it best
  Nobody else is doing it`

Padlock

Padlock is Suite of Security Technologies

Privacy
- •Hardware Random Number Generator (RNG)
- •Advanced Cryptography Engine (ACE)
  - •AES encryption support
  - •Secure Hash Algorithm (SHA-1/256)
  - •Montgomery Multiplier (RSA acceleration)

Protection
- •Memory Protection-NoExecute (NX)

■VIA is providing security primitives. Not Policies.

Padlock

	RNG Random Number Generator	ACE Advanced Cryptography Engine
High Quality	• Hardware based • Quality vs bit rate load option • Designed for Verification and Test	• AES Encryption - US Gov. standard ▪ 128,192,256 bit key length • Secure Hash Algorithm ▪ SHA-1,SHA-256 • Montgomery Multiplier ▪ RSA multiplication up to 32k! Key sizes. • Integrated into CPU
High Performance	• High Bit Rate->750kbps @ best quality • Asynchronous Multi-Byte Generation	• AES ▪ Up to 12.8 Gigabits per second with 1 GHz ▪ Fastest CPU (3.0 GHz Pentium 4) with Fastest Algorithm is only 1.5 Gbps • Montgomery Multiplier • 1024-bit RSA SSL ops
Efficient and Secure Programming Interface ▪ Application/End user level access ▪ Transparent to Operating System ▪ Inherent multitasking		

Padlock Cryptography Applications

Existing Implementations

Operating System CryptoAPI

Encrypted File System

Dark Networks

Pretty Good Privacy

GNU Privacy Guard

PKZip, WinZip

Hard Disk Scrubber

Environments

Banking

Government

Point of Sale Terminals

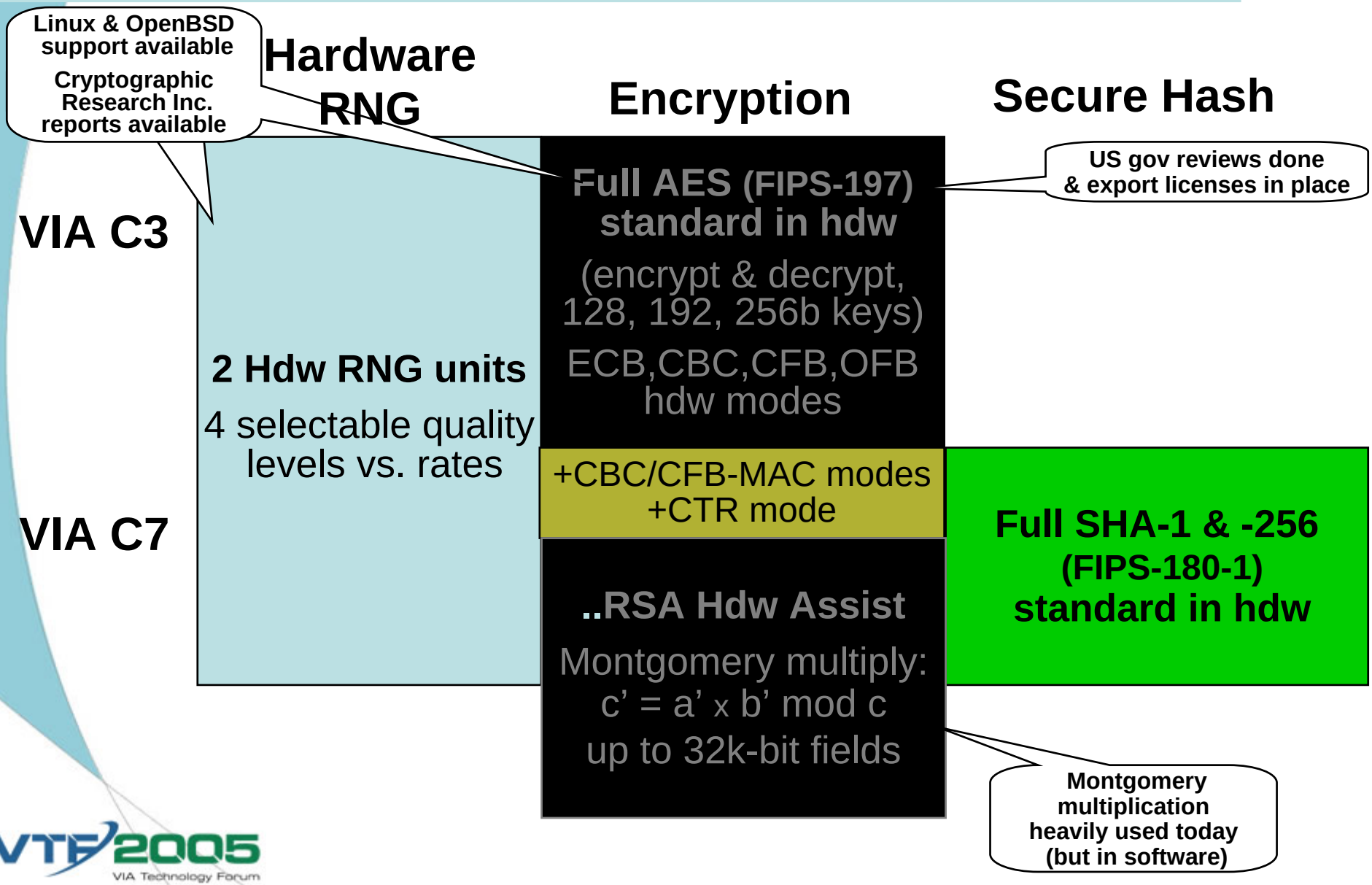
Wireless

Routers

Peer-to-Peer Networking

VPN

Our Security Implementation



Our Security Implementation

also see
fp.gladman.plus.com
for his numbers...
“spectacular performance”

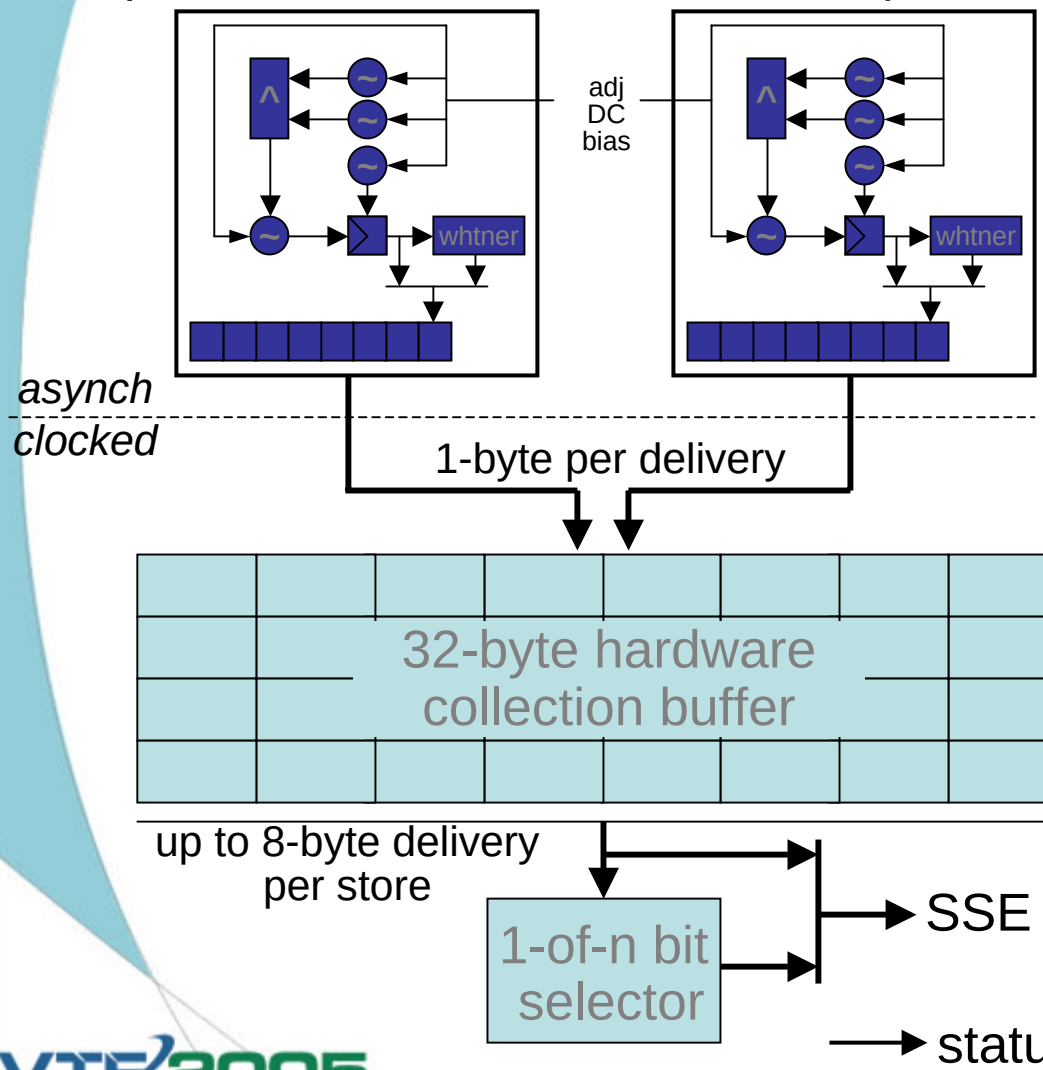
	Ha…	…ption	Secure Hash
VIA C3	**1.6-60 Mbs rate** (depending on desired quality)	1 clk/round/128 bits **≈25 Gbs peak** (2 GHz processor, 128b key)	**Measured Decrypt** **64 KB file** **1.3 GHz VIA C3: ≈ 10.94 Gb** **3.0 GHz P4: ≈ 0.78** **6.4 MB file** **1.3 GHz VIA C3: ≈ 1.65** **3.0 GHz P4: ≈ 0.78**
VIA C7	Same + ≈70x rate of best quality mode (running bits thru SHA hash)	128b x 32b mod(x) =16 clks full a x b mod(m) < $4n^2$+(≈3)n K clks (n = bit leng/K) **>= 800 1K RSA ops/s** (OpenSSL, priv key, 2 GHz)	SHA-1:1 clk/rnd/512b SHA-256: 2 clk/rnd/512b **≈12 Gbs peak** (SHA-1, 2 GHz processor)

Can’t achieve RNG quality in SW

vs. measured OpenSSL
1.3 GHz VIA C3: ≈ 50
3.0 GHz P4: ≈ 256

Nehemiah Hardware RNG

2 duplicate RNGS in different areas (& rotated)



Features

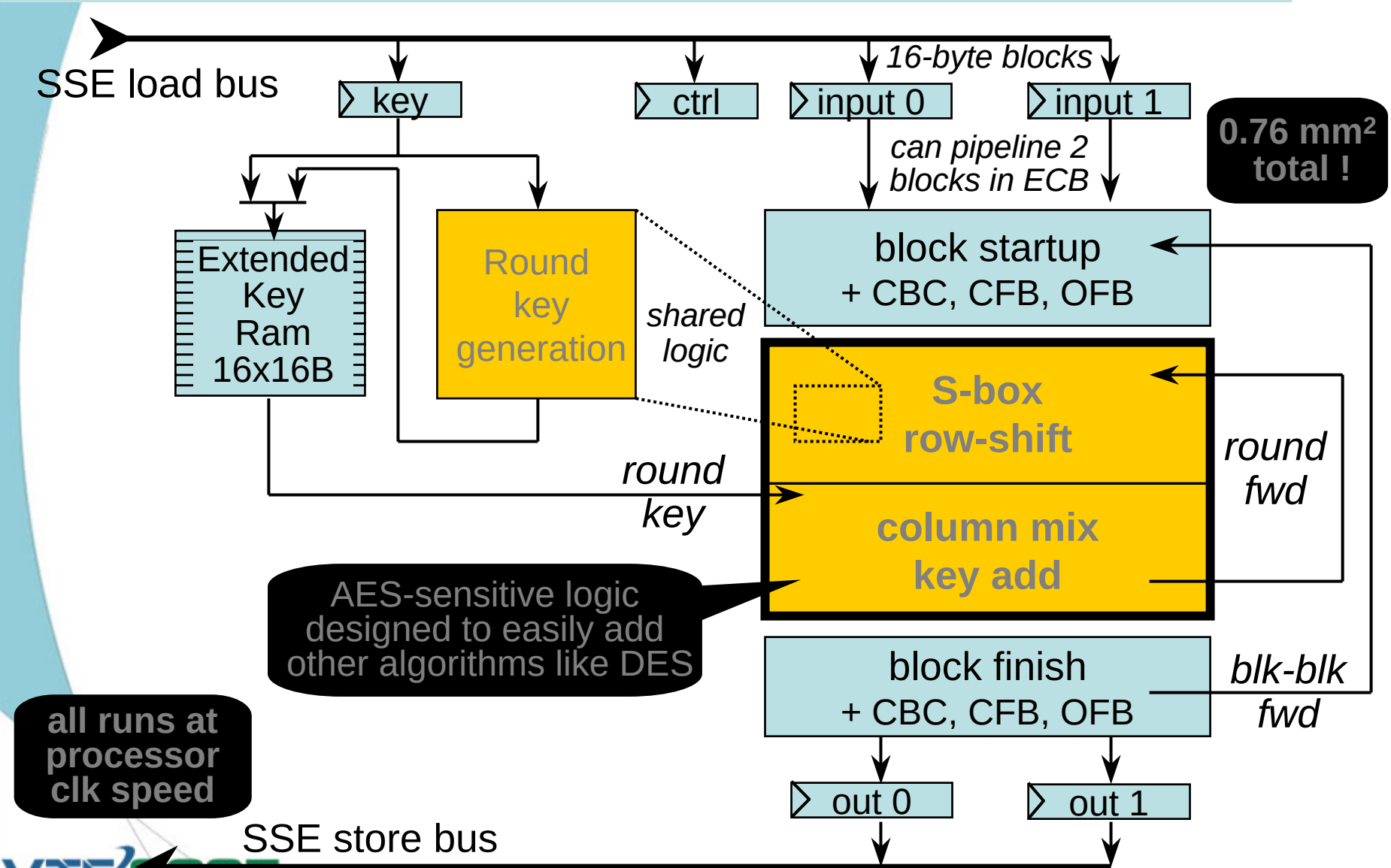
- *Hardware generation*
- *Non-privileged interface*
- *Wide range of speed vs. "quality": 1.6–60 Mbs*
- *Asynch generation (minimal sw overhead)*
- *Inherent multi-tasking*
- *Already Supported in Linux & BSD*
- *Extensive statistical analysis provided (public report from Cryptographic Research Inc.)*

hdw | *sw*

(rep)store-RNG

new x86 instruction

Advanced Cryptography Engine



The Full Monty

To perform $C = A^N \bmod(M)$,
a series of $C_{i+1}=(C_i \times C_i)[\times A]$ is performed

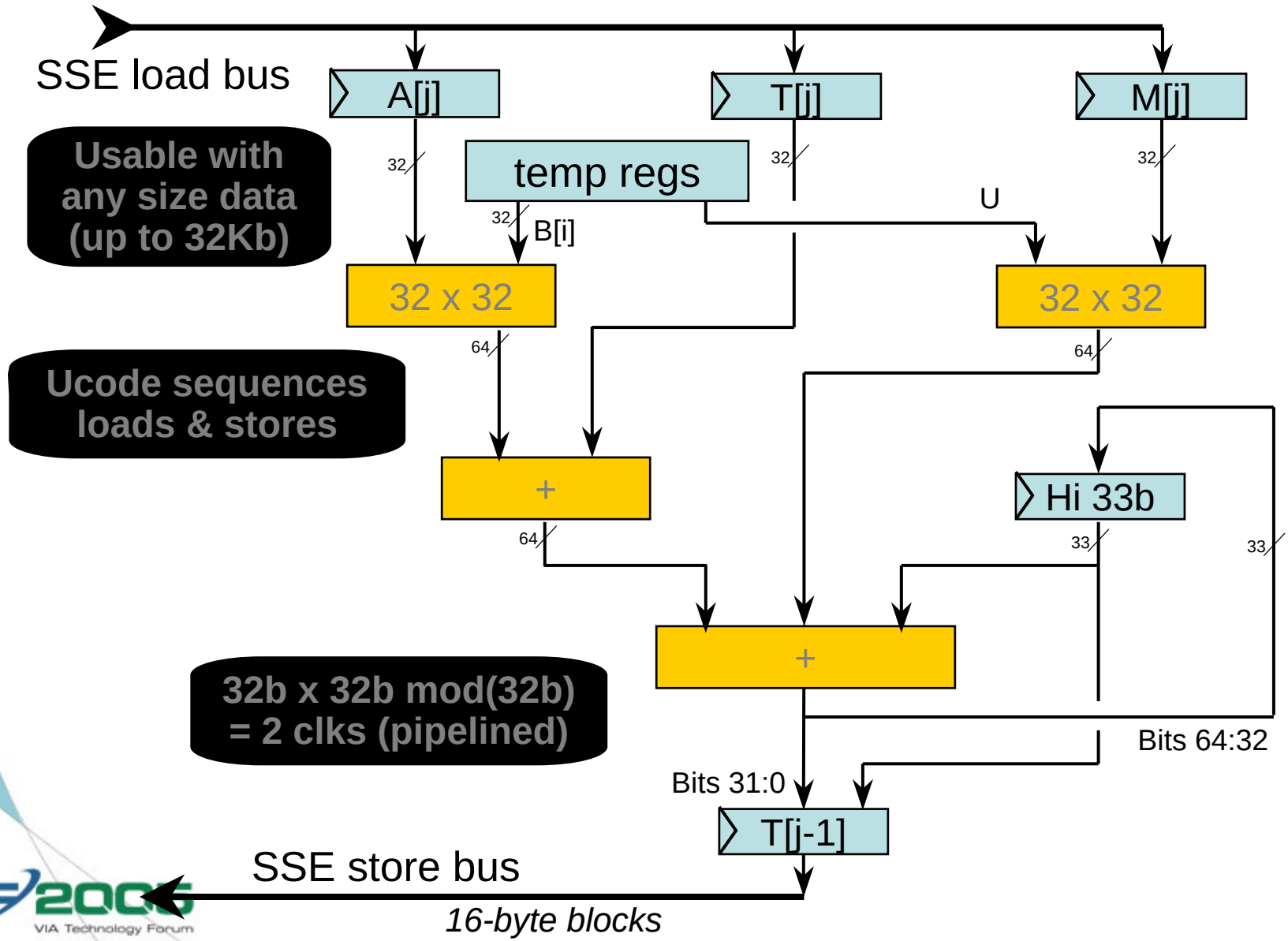
1. Transform A into Montgomery residue space
   A' = MontMul(A,Rm,M)
   (Rm is 2^u Mod(M), u is number bits in M)
2. Perform $C_0'=A'xA'$
   C_o' = MontMul(A',A',M)
3-n. Perform series of
   $C_{i+1}'(C_i'xC_i')[x A']$
   C_{i+1}' = MontMul(C_i',C_i',M)
   [C_{i+1}' = MontMul(C_{i+1}',A',M)]
n. Transform result back to real number space
   C = MontMul(C_{i+1}',1,M)

The Secret

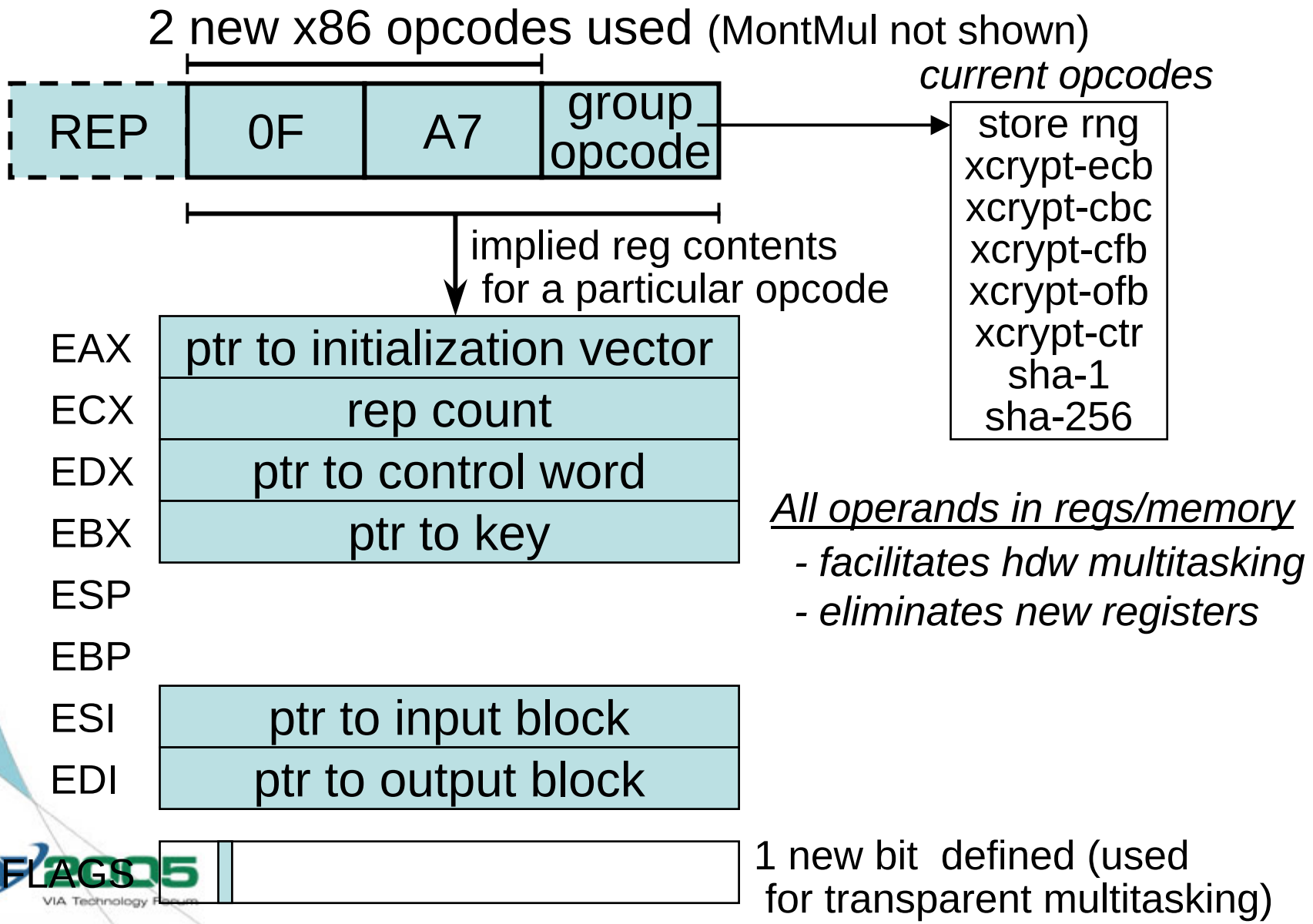
MontMul() algorithm is almost as fast as normal multiply algorithm,

vs. "mod" operation, which requires a divide

VIA C7 Montgomery Multiplier



Padlock Security x86 ISA



All operands in regs/memory

- *facilitates hdw multitasking*
- *eliminates new registers*

Final Thoughts - Performance

- Who is the World's fastest Man?

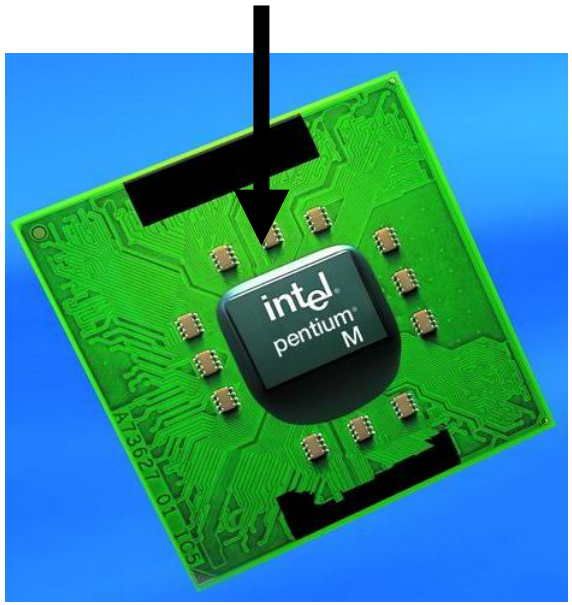
Tim Montgomery -100m Dash World Record Holder?

Paul Tergat – Marathon World Record Holder?

Final Thoughts - Performance

Intel Pentium-M

87mm^2
die size



VIA C7-M

30mm^2
die size